RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: FRP-W01

Guardians of the Cyber Galaxy: Allies Against AI-Powered Cybercrime

MODERATOR:

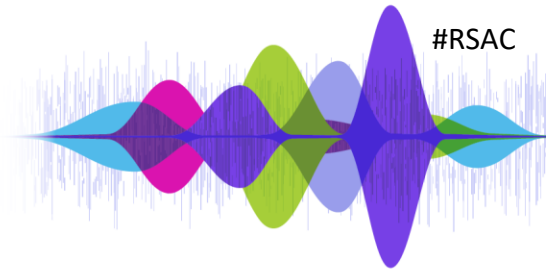
Garylene (Gage) Javier
Counsel
Privacy & Cybersecurity
Crowell & Moring LLP

PANELISTS:

Sean Farrell
Lead Counsel, AI Strategy, Digital Crimes Unit
Microsoft Corporation

Andrew Sczygielski
Supervisory Special Agent
Federal Bureau of Investigation

Craig Jones
Immediate Past Director Cybercrime
INTERPOL



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

#RSAC

Many Voices.
One Community.

MODERATOR:

Garylene (Gage) Javier

Counsel
Privacy & Cybersecurity
Crowell & Moring LLP

PANELISTS:

Sean Farrell

Lead Counsel, AI Strategy
Digital Crimes Unit
Microsoft Corporation

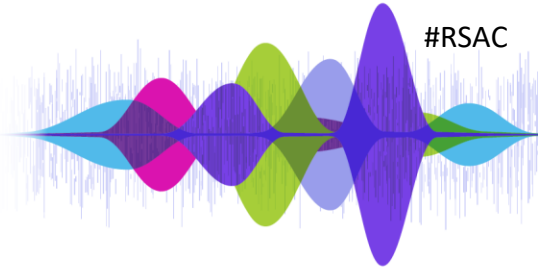
Craig Jones

Immediate Past Director
Cybercrime
INTERPOL

Andrew Sczygielski

Supervisory Special Agent
Federal Bureau of Investigation

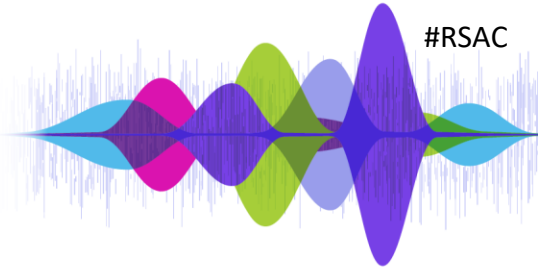
AI in Cybercrime



95%	Costs saved by spammers using LLMs for phishing emails
20,254	AI-generated CSAM images posted to a forum in 1 month
$15k	Amount lost by a victim to an AI voice cloning attack
85%	Identity fraud cases using AI to create fraudulent identities
40%	Phishing emails targeting businesses that are AI-generated

Source: Cobalt, DHS, McAfee

Combatting AI-Powered Cybercrime



Trigger — Attackers are evolving in complexity and are using AI in cybercrime

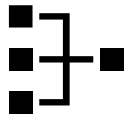
Effect — Usual tactics to defend are no longer effective

Issue — Organizations and law enforcement need better strategies to fight back

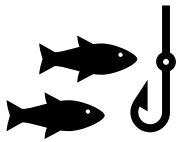
Solution — Public and private sectors should collaborate to fortify defenses against AI-powered cybercrime

AI-Powered Cyber Threats

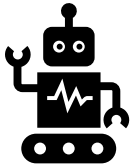
- Malicious activities using AI to increase **effectiveness**, **scale**, and **sophistication**
- **Automates** attacks and **adapts** in real-time
- More **efficiently** evades detection and exploits vulnerabilities



Botnet



Enhanced Phishing Attacks



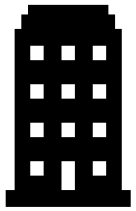
Automated Vulnerability Exploitation

Deepfake Videos and Audios

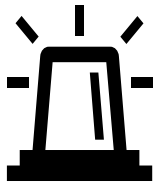
Social Engineering

Smart Malware

Public-Private Partnerships



Private Sector



Law Enforcement

International Stakeholders and Public Entities

- Collaboration between **government agencies** and **private sector** entities
- **Sharing** of information, resources, and expertise
- Develop strategies to prevent, detect, and mitigate cybercrime **collectively**
- **Improve** threat intelligence
- **Enhance** incident response capabilities

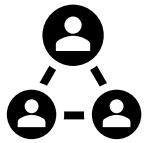
Strategies on Detection, Defense, and Collaboration

Complexity of AI Detection

Awareness of Government Positions & Policies

Protection of Sovereign Data

Affirmative Litigation



Connections with Lesser-Known Resources

Education of Strategies

Apply What You Have Learned Today

Immediate Takeaway Actions

- Establish contact with local FBI field office.
- Review organization policies on parameters for external collaboration and consult legal team on outreach guidance.
- Evaluate AI resources.

Actions to Implement Within 3 Months

- Conduct a thorough assessment of current cybersecurity measures against AI-driven threats.
- Develop a strategy for integrating AI tools to enhance threat detection and response capabilities.
- Participate in opportunities like tabletop exercises on AI that combine experts to address scenarios.
- Organize training sessions for staff on recognizing and responding to AI-enabled cyber attacks.
- Initiate partnerships with external cybersecurity organizations for shared threat intelligence.

RSAC 2025 Conference

Many Voices.
One Community.

For more information:

Email Gage Javier at gjavier@crowell.com